Protecting “Personal Clouds” with UMA and OpenID Connect

@UMAWG
#UMApcloud for questions
19 June 2014
tinyurl.com/umawg for slides, recording, and more
The marvelous spiral of controlled personal data sharing

Further reading: tinyurl.com/umawg
Agenda

• The realities and challenges of personal data sharing
• “UMA for humans 101”
• A walk through personal cloud models
• Use cases
• How UMA leverages OpenID Connect – with demo
• Next steps

Thanks to MIT-KIT for sponsoring this webinar and taking part!

Thanks to Kantara for supporting the UMA work!

Thanks to our additional webinar participants!
The realities and challenges of personal data sharing
What is personal data?

Personal Data is the **Life Blood** of the Information Age

Personal Data is the New “**Oil of the Internet**”

Personal Data is the new **currency**
Ways to measure the value of personal data

- Market capitalization
- Revenue per record/user
- Market Price
- Cost of data breach
- Pay to protect

\[ \text{USD} \quad \frac{112}{40} \text{ per user record} \]

\[
\begin{align*}
\text{Street address} & \quad \text{USD} \quad 1.7 \\
\text{Data of Birth} & \quad \text{USD} \quad 0.5 \\
\text{Social Number} & \quad \text{USD} \quad 1.7 \\
\text{Military record} & \quad \text{USD} \quad 30 
\end{align*}
\]

Data breach cost $171M
USD 1.7 per record

72% of European citizens are concerned that their personal data may be misused...

Individuals have little visibility into the practices of the organizations they are putting their trust in – until their data is breached or misused.

Risks: Loss of Trust
The “personal data price” for online service is too high: typing…

• Provisioning by hand
• Provisioning by value
• Oversharing
• Lying!
The “personal data price” for online service is too high: connecting...

- Meaningless consent to unfavorable terms
- Painful, inconsistent, and messy access management
- Oblivious oversharing
The “personal data price” for online service is too high: private URLs...

- Handy but insecure
- Unsuitable for really sensitive data
“UMA for humans 101”
UMA turns online sharing into a privacy-by-design solution

The “user” in User-Managed Access (UMA)

Further reading: tinyurl.com/umapbd
UMA turns online sharing into a privacy-by-design solution
UMA turns online sharing into a privacy-by-design solution

I want to share this stuff selectively
- Among my own apps
- With family and friends
- With organizations

I want to protect this stuff from being seen by everyone in the world

I want to control access proactively, not just feel forced to consent over and over
UMA turns online sharing into a privacy-by-design solution

- Standardized APIs for privacy and "selective sharing"
- Outsources protection to a centralized "digital footprint control console"
A walk through personal cloud models
Personal data ecosystem emerging trends
Mapping UMA to personal clouds and life management platforms

Access Requesting Party

Informed Pull

Controlled Push

Data Stores

Data Control

LMP

Home

Bank

Healthcare

Car
Mapping UMA to personal clouds and life management platforms

Data Stores

LMP
UMA AS

Requesting Party

Healthcare

Bank

Home

Car
Mapping UMA to personal clouds and life management platforms

- **Resource Owner**
- **LMP**
- **Requesting Party**
- **Client**
- **Data Stores**

- **manage**
- **consent**
- **protect**
- **negotiate**
- **authorize**
- **access**

- **Bank**
- **Healthcare**
- **Home**
- **Car**
Use cases
Case studies for...

- Management and sharing of personal accessibility needs and preferences
- Secure sharing of university e-transcripts
- Healthcare relationship locator service and patient-centric consent directives
- Access management 2.0 for the enterprise (previous webinar)
- ...
- Protecting the personal data stores of everyone at MIT

Further reading: tinyurl.com/umacase
Protected personal data stores: MIT’s view

1. User-generated data (mobile devices)
2. Student Alice (owner of PDS)
3. Privacy-Preserving Queries and BigData access (authorized by Alice)
4. Data-item Sharing with Authorization from Alice (e.g. calendar access)
How UMA leverages OpenID Connect
Use case:
Transcript of Records sharing

• Student interacts with an online job application system
• Student fills in a job application form and provides:
  – Personal information
  – Transcript of Records document
• Data is transferred from the student’s personal data service
  – With explicit consent
• Employer requests access to additional data
  – …and this has to be confirmed by the student

“Sharing Trustworthy Personal Data with Future Employers”
http://kantarainitiative.org/confluence/display/uma/cv_sharing_scenario
UMA model

- resource owner
- authorization server
- requesting party
- client

- manage
- protect
- authorize
- access
- control
- consent
- negotiate
- manage
Scenario (Peter sharing data)

- **Resource Owner**
  - Manage
  - Control
- **Consent**
- **Negotiate**
- **Requesting Party**
  - Manage

**Personal Data Service**
- Personal Information
- Transcript of Records

**Access**
- **Authorize**

**Requesting Party**
- Peter (Student, Job Seeker)

**Access**
- CareerMonster
- Job Positions
Scenario (Tom accessing data)

- **resource owner**
- **consent**
- **control**
- **manage**
- **protect**
- **authorize**
- **negotiate**
- **requesting party**

**Personal Data Service**
- Personal Information
- Transcript of Records

**Phone Number**

**requests**
- Peter (Student, Job Seeker)
- Tom (Employer)
Live demo
NuveAM – Authorisation Manager

• UMA-compliant Authorisation Server (AS) from Cloud Identity Limited:
  – Access control to data in the Cloud
  – API security management
  – Real-time monitoring and audit

• Use cases: **Securing Cloud-based Personal Data Services (PDS);** Managing access to Cloud-based APIs

• Uses open standards, including: UMA, OAuth 2.0, OpenID Connect, SAML 2.0

• Open source frameworks: Java and Python

http://www.cloudidentity.co.uk/products/nuveam
Nuve User-Managed Access

![Diagram showing Nuve User-Managed Access integration with various social login and identity verification methods, along with supported Open Standards and third-party applications.]
UMA claims-based authorisation

- UMA allows for the use of claims to support Claim-Based Access Control (CBAC):
  - Trusted claims from Trusted Third Parties
  - Self-asserted claims
- In CBAC, the decision to grant access to a protected resource is made based on Subject’s information/attributes, such as name, age, email address, role, location, credit score, etc.
- …or a Subject’s statement (e.g. promise to adhere to licensing terms)
OpenID Connect role in UMA

• OpenID Connect (OIDC) provides authentication, consented attribute sharing, and attribute transmission capability

• OIDC allows third-party asserted claims from distributed sources to be collected

• UMA leverages OIDC in claims-gathering flow in one of two ways:
  – AS interacts directly with requesting parties, or
  – indirectly via clients
UMA AS Collecting Claims from Requesting Party

Client redirects the Requesting Party to AS
Generic UMA Model

UMAN
MANAGEMENT AS
policy decision
Point

Control

Protect

Authorize

Manage

Resource Owner

UMA AS

Resource Server

Protected Resource

Access

Client

SSO

Requesting Party

OpenID Domain

UMA Domain

Resource Owner

UMA AS

policy decision
Point

Control

Protect

Authorize

Manage

Resource Owner

Resource Server

Protected Resource

Access

Client

SSO

Requesting Party

OpenID Domain

UMA Domain
Client application conveying claims to UMA AS

1. Request
2. AuthN
3. Access_token
4. Request Userinfo
5. Userinfo

Requesting Party

OpenID Connect AS

UserInfo EndPoint

SSO

OpenID Domain

UMA Domain

Resource Owner

UMA AS

policy decision Point

Control

Protect

Authorize

Manage

Resource Server

Protected Resource

Access

Client

Protected Resource

OIDC Client
UMA AS acting as Claims Client
UMA AS acting as Claims Client

UMA AS can collect additional claims from internal user store

This can be a SAML-compliant IDP just as well
Next steps
Next steps for the WG…and you

• Get involved!
  – Become an “UMAnitarian” (it’s free)
  – Participate in the interop and our implementation discussions
  – Follow and engage with @UMAWG on Twitter

• Current work:
  – Technical: claim profiling and core spec variations
  – Business: access federation trust frameworks

• Stay tuned for a webinar on UMA and Healthcare in Q3
Questions? Thank you!

@UMAWG
#UMApcloud for questions
19 June 2014
tinyurl.com/umawg for slides, recording, and more